REMARKS

Claims 1-11, 13 and 22-110 are pending. In this Response, claims 1-11, 13, 26, 61 and 73 have been amended, and claims 12 and 14-21 have been cancelled.

I. CLAIM OBJECTIONS

Claims 26 and 61 are objected to since "detect" should be "defect." Applicant agrees, and notes with appreciation the Examiner's helpful suggestions. Accordingly, claims 26 and 61 (and 73) have been amended to recite "defect" instead of "detect." Therefore, Applicant requests that these objections be withdrawn.

II. SECTION 112, SECOND PARAGRAPH REJECTION

Claim 61 is rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In particular, "the media detect list" lacks antecedent basis. Applicant agrees, and as mentioned above, claim 61 has been amended to recite "defect" instead of "detect." Therefore, Applicant requests that this rejection be withdrawn.

III. SECTION 102 REJECTIONS – DURST, JR. ET AL.

Claims 1-2, 5, 7, 10-12, 14, 16, 18 and 20 are rejected under 35 U.S.C. § 102(b) as being anticipated by *Durst, Jr. et al.* (U.S. Patent 5,113,518).

Durst, Jr. et al. discloses a method for preventing unauthorized use of software. The software is stored on a mass memory device such as floppy disk, magnetic tape, ROM cartridge or CD ROM. The software includes an authorization program and an applications software program, and the authorization program includes a set up procedure (FIG. 13A) and an authorization procedure (FIG. 13B). The set up procedure determines and stores a signature of a computer system. Thereafter, whenever the software is executed, the authorization procedure obtains the signature of the computer system, compares the signature to the stored signature, and allows the applications software program to execute on the computer system if the signatures match.

Durst, Jr. et al. makes clear that the applications software program is not combined with or altered by the signature:

> As mentioned above, the present invention limits execution of an applications software program to the particular computer system whose signature corresponds to the signature of an authorized computer system. It is expected that the applications software program is stored on a mass memory device, such as a floppy disk. Also stored on this floppy disk is an authorization program which, typically, carries out the following functions: The authorization program measures and stores the signature of the computer system on which it first is installed. Thereafter, whenever the applications program is to be used, the authorization program first measures the signature of the computer system which is intended to use the applications software program, compares the measured signature to the stored signature and then enables the applications software program to be "run" only if the measured and stored signatures are substantially the same. (Col. 11, lines 11-29).

Claim 1 as amended recites "the host processor combining the source content to be secured with the source fingerprint to generate the fingerprinted content; and the host processor instructing the source storage medium to store the fingerprinted content." *Durst, Jr. et al.* fails to teach or suggest that the computer system stores a fingerprinted content that is generated by combining the applications software program with the signature. Instead, the computer system executes the applications software program if the authorization program determines that the signatures match. Claims 2, 5 and 7 depend (directly or indirectly) from claim 1.

In sustaining these rejections, the Examiner states as follows:

> As to claim 1, Durst discloses a method and system for preventing unauthorized use of software comprising determining a source fingerprint from the source storage medium (col. 3, lines 35-57, i.e. signature of the computer system derived from disk drive parameter), wherein the source fingerprint is a physical attribute of the source storage medium (col. 9, lines 3-35); combining the source content (i.e. applications software program) to be secured with the source fingerprint (i.e. authorizing program storing signature of the computer system which comprising signature of the source storage medium) to generate the fingerprinted content (col. 11, lines 15-21) and instructing the source storage medium to store the fingerprinted content.

As best Applicant understands, the Examiner asserts that *Durst, Jr. et al.* discloses determining a source fingerprint (stored signature) from a source storage medium (disk drive), combining a source content (applications software program) with the source fingerprint (stored signature) to generate a fingerprinted content (applications software program and stored signature) and instructing the source storage medium (disk drive) to store the fingerprinted content.

Unfortunately, the Examiner has not even attempted to explain how *Durst, Jr. et al.* instructs the source storage medium (disk drive) to store the fingerprinted content (applications software program and stored signature). More importantly, this operation does not happen. Although the authorization program with the stored signature allows the applications software program to be transferred from the mass memory device to the disk drive if the measured signature matches the stored signature, the authorization program with the stored signature remains stored on the mass memory device. Moreover, transferring the stored signature to the disk drive would enable the computer system to crack the authorization program and pirate the applications software program. This would defeat the purpose the authorization program, thereby rendering *Durst, Jr. et al.* unsatisfactory for its intended purpose.

Under 35 U.S.C. §102, anticipation requires that each and every element of the claimed invention be disclosed in the prior art. *Akzo N.V. v. United States International Trade Commission*, 1 USPQ 2d 1241, 1245 (Fed. Cir. 1986), *cert. denied*, 482 U.S. 909 (1987). That is, the reference must teach every aspect of the claimed invention. M.P.E.P. § 706.02.

Claim 10 has been amended as claim 19 rewritten in independent form including all limitations of the base claim and any intervening claims, which the Examiner indicated as allowable.

Claim 11 has been amended as claim 21 rewritten in independent form including all limitations of the base claim and any intervening claims, which the Examiner indicated as allowable.

Claims 12, 14, 16, 18 and 20 have been cancelled.

Therefore, Applicant requests that these rejections be withdrawn.

IV. SECTION 103 REJECTION – NARASIMHALU AND DURST, JR. ET AL.

Claim 1 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Narasimhalu* (U.S. Patent 5,412,718) in view of *Durst, Jr. et al.*

Durst, Jr. et al. fails to teach or suggest instructing the source storage medium to store the fingerprinted content, as mentioned above.

Therefore, Applicant requests that these rejections be withdrawn.

V. SECTION 103 REJECTIONS – DURST, JR. ET AL. AND SCHNEIER

Claims 3-4 and 6 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Durst, Jr. et al* .in view of *Schneier* (Applied cryptography).

Durst, Jr. et al. fails to teach or suggest instructing the source storage medium to store the fingerprinted content, as mentioned above.

Therefore, Applicant requests that these rejections be withdrawn.

VI. SECTION 103 REJECTION – DURST, JR. ET AL. AND NARASIMHALU

Claims 8-9 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Durst, Jr. et al.* in view of *Narasimhalu.*

Claim 8 has been amended as claim 15 rewritten in independent form including all limitations of the base claim and any intervening claims, which the Examiner indicated as allowable.

Claim 9 has been amended as claim 17 rewritten in independent form including all limitations of the base claim and any intervening claims, which the Examiner indicated as allowable.

Therefore, Applicant requests that these rejections be withdrawn.

VII. OTHER AMENDMENTS

Claims 1-7 have been amended to improve clarity. No new matter has been added.

Claim 13 has been amended to be rewritten in independent form including all limitations of the base claim and any intervening claims, which the Examiner indicated as allowable.

VIII. FEES

The fee is calculated below:

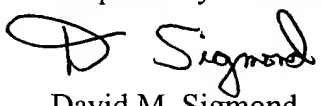
For	Claims Remaining After Amendment	Highest Number Previously Paid For		Extra Claims	Rate		Additional Fee
Total Claims	101	– 110	=	0	x $50	=	$0
Independent Claims	14	– 9	=	5	x $200	=	$1000
Multiple Dep. Claim	0	0			$360	=	$0
Total Fee						=	$1000

Please charge the $1000 fee and charge any underpayment and credit any overpayment to Deposit Account No. 13-0016/Q00-1000-US1.

IX. CONCLUSION

In view of the remarks set forth herein, the application is believed to be in condition for allowance. Should any issues remain, the Examiner is encouraged to telephone the undersigned attorney.

Respectfully submitted,



David M. Sigmond
Attorney for Applicant
Reg. No. 34,013
(303) 702-4132
(303) 678-3111 (fax)